 https://doi.org/10.24191/jeesr.v29i1.014

Implementation and Performance Evaluation of GRE over IPsec for Secure ASTERIX Radar Communications over XSatcom Networks

Muhammad Hazwan bin Abd Lateb, Nur Nabila binti Mohamed, and Yusnani binti Mohd Yussoff*

Abstract— **Modern air defence systems rely on secure and efficient communication networks to ensure timely data transmission and operational effectiveness. This study evaluates the system performance of an air defence network by simulating an XSatcom IP environment in GNS3, comparing an unsecured tunnel (GRE-only) with a secured tunnel using GRE over IPsec. The primary objectives include designing a secure network configuration in GNS3, simulating communication between two radar sites and a Command Operations Center (COC), and assessing data confidentiality and performance through delay and throughput metrics. Results indicate that while encryption introduces minimal overhead, the impact on delay and throughput is negligible, ensuring efficient data transmission. Additionally, the GRE over IPsec configuration significantly enhances the security of ASTERIX data exchanges, demonstrating its suitability for secure air defence communications. The findings confirm that GRE over IPsec provides an optimal balance between performance and security for critical military networks.**

Index Terms—**Air Defence System, GNS3, GRE over IPsec, IPsec, XSatcom.**

I. INTRODUCTION

A national air defence system stands as the cornerstone of a nation's security infrastructure, playing a pivotal role in safeguarding its airspace and ensuring the protection of its citizens, critical assets, and territorial security [1-2]. The primary purpose of such a system lies in its ability to detect, monitor, and respond to potential aerial threats, ranging from unauthorized aircraft incursions to hostile missile attacks. This system integrates radar surveillance, command and control centres, interceptor missiles, and anti-aircraft artillery to provide a comprehensive shield over strategic areas. By maintaining continuous situational awareness and a rapid response capability, an air defence system ensures the safety of a nation's airspace.

In the domain of air defence systems, the dependence on terrestrial networks for the seamless communication and fusion of sensor data from multiple radar sources has long served as the bedrock of operational efficiency and security. However, the critical need for continuous connectivity combined with the vulnerabilities inherent in land-based networks necessitates a robust alternative solution. This necessity arises from various factors, including the susceptibility of land-based networks to natural disasters, infrastructure failures, or deliberate attacks, all of which could lead to service disruptions with potentially severe ramifications.

In 2015, the national armed forces procured the X-band satellite communication (XSatcom) system, which provided strategic capabilities expansion to the armed forces toward full network coverage in the region for efficient command and control as well as better interoperability [3]. The XSatcom system operates with a transponder on the geostationary (GEO) satellite MEASAT-3B, which was successfully launched on 14 September 2014 [4]. This technology has significantly enhanced communication capabilities, especially for military operations in remote or challenging terrains. Currently, the XSatcom system is mainly operated, managed, and controlled by the Satellite Communication Centre (SCC) in a designated military camp.

The uninterrupted operation of air defence surveillance systems is critical, yet terrestrial IP networks face limitations in reliability and coverage. While adopting XSatcom as a backup communication channel addresses redundancy concerns, it introduces new security vulnerabilities. Without robust encryption, the system remains exposed to cyber threats like data breaches and man-in-the-middle attacks, jeopardizing the integrity of radar surveillance data transmitted between remote sites and command centers.

To mitigate these risks, this study proposes integrating Generic Routing Encapsulation (GRE) with IPsec encryption within the XSatcom network, a commonly used solution in IP networks. GRE creates logical tunnels for packet encapsulation, while IPsec provides confidentiality, authenticity, and integrity. This combination safeguards ASTERIX radar data from unauthorized access or tampering. The solution is evaluated through a simulated XSatcom environment in GNS3, where network performance (delay, throughput) and security efficacy are tested under a topology replicating two radar sites and a Command Operations Centre (COC).

This manuscript is submitted on March 13, 2026, revised on August 14, 2026, accepted on September 03, 2026 and published on October 31, 2026.

Muhammad Hazwan bin Abd Lateb, Nur Nabila binti Mohamed, Yusnani binti Mohd Yussoff are with Faculty of Electrical Engineering, Universiti Teknologi MARA, 40450 Shah Alam, Selangor, MALAYSIA. (e-mail: azlindaaziz@uitm.edu.my)

*Corresponding author
Email address: yusna233@uitm.edu.my

1985-5389/© 2026 The Authors. Published by UiTM Press. This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/).

II. Related Work

In the domain of satellite communication, numerous studies have investigated the security and performance implications of network tunnelling protocols, particularly in high-latency environments. Firmansyah et.al conducted a detailed Quality of Service (QoS) analysis on a Thuraya GEO satellite communication system using UDP transmissions, both with and without Virtual Private Network (VPN) configurations [5]. The study reported an average delay of 1.12 seconds when VPN was enabled, highlighting the encryption overhead.

Romain et al. evaluated the performance of VPN protocols WireGuard and OpenVPN across multiple satellite deployment scenarios, including both GEO and LEO topologies [6]. Their comparative study provided insights into deployment flexibility and the adaptability of encryption mechanisms. Pedersen et al. extended this exploration with a comprehensive threat analysis of GEO-based satellite networks, identifying 15 security vulnerabilities and recommending VPN adoption as a key mitigation strategy [7].

Focusing specifically on tunnelling methods, Ogudo compared GRE and GRE over IPsec in public network environments, noting that GRE alone lacks encryption, whereas GRE over IPsec significantly enhances data security through payload encryption [8]. Li & Zhou simulated GRE over IPsec in GNS3 to construct a secure VPN tunnel and confirmed its reliability in protecting data in transit [9]. Supporting this, Penaflor et al. successfully demonstrated cost-effective secure interconnectivity between remote office sites using GRE over IPsec [10]. Likewise, Uddin et al. simulated the use of GRE over IPsec to enable IPv4 data transfers over IPv6 WAN environments [11].

In studies focused on VoIP and QoS, Budiyanto et al. [12] tested multiple VPN protocols, including GRE over IPsec, examining delay, jitter, packet loss, and throughput. The results confirmed GRE over IPsec's suitability for VoIP under proper configuration. Alausa et al. further examined GRE over IPsec with various codecs over IPv4 and IPv6, revealing that codec choice critically influences tunnel performance [13].

He et al. (2023) simulated GRE over IPsec tunnels in a point-to-multipoint (P2MP) satellite configuration to support both unicast and multicast traffic [14]. Murariu & Ciotirnae compared GRE, GRE over IPsec, plain IPsec, and DMVPN in VoIP applications, finding all to meet performance benchmarks, though IPsec-based configurations incurred higher processing costs [15]. Budiyanto & Silalahi [16] also compared GRE over IPsec with IPIP, concluding that IPIP offered slightly better performance due to lower overhead, albeit without encryption.

On the hardware front, Stankovic et al. [17] implemented GRE tunnelling on low-cost System on Module (SoM) devices, suggesting its potential for budget-sensitive secure networking. Mahmmod et al. [18] proposed FPGA-based parallel processing for IPsec to improve encryption throughput, while Xu & Ni [19] highlighted the efficiency and transparency of IPsec in VPN deployment. Hashiyana et al. demonstrated that IPsec can provide a cost-effective internal VPN solution, as seen in their implementation at the University of Namibia [20].

Network protocol performance over secure links was explored by Basit et al., who showed that EIGRP outperforms OSPF in convergence and failover response over IPsec-encrypted networks [21]. Darmawan et al. compared L2TP/IPsec and SSL protocols in VoIP scenarios, identifying SSL as better in overall QoS but L2TP/IPsec as superior for jitter handling [22]. For hybrid approaches, Juma et al. [23] integrated IPsec with OpenSSL for IoT VPN security, balancing transparency with increased bandwidth cost.

Ethernet over IP (EoIP) based studies include Nurhaida & Ngadiyono and Dharma [24-25], who applied EoIP over IPsec to static routed VPNs, reporting better delay and packet loss performance despite slightly reduced throughput. Haris et al. [26] suggested that EoIP/IPsec could be integrated into secure electric vehicle communications, despite its proprietary constraints. Thein conducted performance analysis on five Layer-2 VPNs (PPP, L2TP, OpenVPN, EoIP, MPLS/VPLS), noting minimal differences in throughput but emphasizing trade-offs between security and flexibility [27]. Similarly, Gaur et al. surveyed Layer-2 VPN protocols, underscoring their relevance to ISPs [28].

Crawshaw provided an overview of VPN development, introducing WireGuard as a modern protocol with simplicity and strong encryption, although its newness may pose compatibility issues [29]. Goyzueta et al. proposed a "Virtual Private Network of Things" (VPNoT), using OpenVPN over Linux on Raspberry Pi for IoT sensor data encryption, validated using TCP dump and Wireshark [30].

Recent studies highlighted the cybersecurity risks affecting satellite communication infrastructures. Kang et al. [31] systematically classified attacks and countermeasures in satellite communication systems according to confidentiality, integrity, and availability requirements. Casaril and Galletta [32] examined vulnerabilities affecting SatCom ground and user segments, particularly satellite modems, routers, and network security controls. Ansong et al. [33] presented a comprehensive cyber-risk assessment for satellite communications and emphasised the need for multilayer security controls across satellite network segments. These recent studies reinforce the need for encryption and secure tunnelling mechanisms when satellite links are used to transmit operationally sensitive data.

Existing research has extensively explored the performance and security implications of network tunneling protocols in satellite communications, with studies such as Firmansyah et al. [5] and Romain et al. [6] quantifying encryption-induced latency in GEO satellite environments. While these works establish a foundation for understanding VPN overhead, they primarily focus on generic VPN applications rather than mission-critical systems like air defence networks. Similarly, Ogudo [8] and Li & Zhou [9] validated GRE over IPsec's security advantages in public networks, but their studies lack evaluation in high-stakes, low-latency contexts where real-time radar data transmission is paramount. Budiyanto et al. [12] and Alausa et al. [13] advanced QoS assessments for VoIP but did not address the unique requirements of ASTERIX data streams in military surveillance. Hardware-oriented studies [17] [18]

optimized cost and throughput but overlooked integration with X-band satellite infrastructure.

Building on the identified research gap, this study evaluates a GRE over IPsec framework specifically for ASTERIX radar data transmitted over XSatcom links. The study addresses three limitations in the existing literature: (1) the trade-off between AES-256 encryption and transmission performance for low-bandwidth radar traffic; (2) the application of secure tunnelling as a redundancy mechanism for military communications when terrestrial links are unavailable or vulnerable; and (3) the evaluation of the proposed configuration using an end-to-end air defence network topology simulated in GNS3.

III. Methodology

To evaluate the effectiveness of securing mission-critical air surveillance data, this study employs a systematic simulation of ASTERIX data transmission over a geostationary (GEO) satellite link. The methodology is designed to quantify the performance trade-offs between an unsecured GRE tunnel and a hardened GRE over IPsec configuration. By replicating real-world military constraints, the approach is divided into three primary phases: system characterization, secure network design, and performance validation.

A. System Characterization

The network is modeled based on the unique requirements of the All Purpose Structured Eurocontrol Surveillance Information Exchange (ASTERIX) protocol, which is the standard for both civil and military surveillance. This study specifically focuses on two critical data categories:

- **CAT 34**: Used for monitoring radar health, system status, and maintenance.
- **CAT 48**: Used for transmitting monoradar target reports essential for aircraft tracking and identification.

To ensure the simulation reflects realistic operational conditions, the environment is constrained by XSatcom parameters, including a one-way delay of 600 ms in each direction and a restricted bandwidth of 2 Mbps. These constraints are introduced via NETEM to evaluate how AES-256 encryption overhead interacts with satellite latency.

Summary of the system specification is tabulated in Table 1.

TABLE 1: SYSTEM CHARACTERIZATION

Payload	The system transmits ASTERIX CAT 34 (monitoring) and CAT 48 (target reports).
Packet Size	1500 Byte Ethernet MTU (prevent fragmentation and delay)
Transmission	Data is sent via UDP multicast to ensure low latency.
Network Design	The topology models transmission from two radar sites to a COC via a simulated satellite (MEASAT 3B)
Security Configuration	IPsec is applied to GRE tunnels using AES-256 encryption, SHA-256 hashing, and pre-shared key authentication.
Constraints	A one-way delay of 600 ms was applied in each direction, and a bandwidth limit of 2 Mbps were introduced via NETEM to replicate realistic XSatcom conditions

Each ASTERIX message is structured according to a User Application Profile (UAP), which defines the data fields to be transmitted. Systems utilizing ASTERIX are uniquely identified using a System Area Code (SAC) and System Identification Code (SIC). These identifiers facilitate consistent communication between diverse surveillance systems and enhance coordination across air traffic control and air defence domains.

B. Secure Network Design

The architecture illustrated in Fig. 1 uses a virtual testbed to interconnect two remote radar sites with a Command Operations Centre (COC) via point-to-point tunnels. The design utilizes GNS3 and VMware to host the following components:

- **Routing & Tunnelling**: OSPF is implemented for unicast routing, while Sparse-Dense mode is used for multicast radar streams.
- **Encryption Layer**: IPsec is applied to the GRE tunnels using the **AES-256** algorithm, **SHA-256** hashing for integrity, and pre-shared keys (PSK) for authentication.
- **Traffic Emulation**: The **Colasoft Packet Player** is used to replay 2,500 authentic ASTERIX packets, while **Sky Display** software provides real-time visual validation of target plots at the COC.

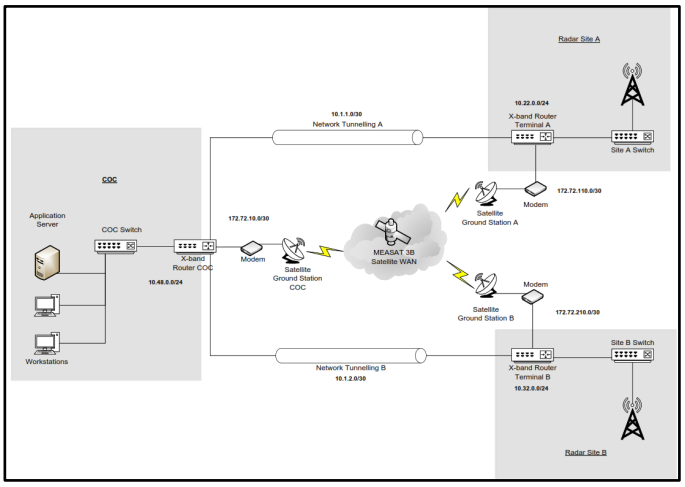


Fig. 1. Network topology.

TABLE 2: SYSTEM AND EXPERIMENTAL CONFIGURATION

Category	Component / Parameter	Specification
Network Architecture	Topology	Two radar sites (RSA, RSB) connected to one COC through two point-to-point GRE tunnels
Routing and Multicast	Protocols	OSPF Area 0 for unicast; PIM Sparse-Dense mode for multicast.
Security Configuration	IKE/IPsec settings	AES-256 encryption, SHA-256 hashing, Diffie–Hellman Group 19, and pre-shared key authentication through ISAKMP.

GRE Tunnel	Tunnel MTU	1414 bytes
Simulation Environment	Software Emulators	GNS3, VMware, and NETEM (for satellite delay).
Satellite Emulation	Link constraints	Bandwidth limited to 2 Mbps with a 600 ms one-way delay.
Traffic Generation	ASTERIX packet replay	Colasoft Packet Player replaying 2,500 authentic ASTERIX CAT 34 and CAT 48 packets.
Performance Testing	Iperf3 configuration	UDP transmission using iperf3 -c 10.48.0.3 -u -b 4000K -t 60, with a test duration of 60 seconds per run.
Test Procedure	Number of runs	Five independent runs under the same network conditions.
Result Reporting	Averaging method	Arithmetic mean of the five independent runs.
Data Visualisation	Verification software	Sky Display for real-time target plot verification.
Computing Resources	Host and virtual machines	Intel i7-8550U with 20 GB RAM; GNS3 VM with 4 CPUs and 4 GB RAM; three Windows 10 node VMs with 1 CPU and 4 GB RAM each

C. Performance Validation

The research methodology employs a multi-tiered validation approach to quantify network performance and verify security efficacy under operational XSatcom conditions. Real-world satellite constraints are emulated using **NETEM** to introduce specific delay and bandwidth parameters.

1) Performance Metrics and Mathematical Models

The study focuses on two primary performance indicators to assess the impact of the GRE over IPsec tunnel:

1. Network Latency (NL): This is defined as the total time required for a packet to travel from the radar site to the COC. Based on the model by Kurose [34], it is calculated as:

$$NL = D_{PR} + D_T + D_Q + D_P \quad (1)$$

where:
D_{PR}: Propagation delay
D_T: Transmission delay
D_Q: Queuing delay
D_P: Processing delay

2. Throughput: This measures the volume of data successfully transferred per unit of time. The calculation follows the standard formula:

$$Throughput = \frac{Total\ data\ transferred\ (bits)}{Time\ taken\ (s)} \quad (2)$$

2) Security and Integrity Assessment Tools

The efficacy of the secure configuration is validated through a combination of packet inspection and real-time surveillance visualization:

- Data Confidentiality: Wireshark is utilized for packet inspection to confirm that Encapsulating Security Payload (ESP) is correctly applied, protecting ASTERIX data from interception.
- Data Integrity: Sky Display software processes decrypted ASTERIX packets in real-time. This visualization of target plots serves as proof that the tunneling process does not compromise data usability or system reliability.

D. Network and Protocol Verification

Before conducting the performance analysis, the integrity of the underlying routing and tunneling infrastructure was validated through specific diagnostic procedures on the COC router to ensure a stable testing environment.

1) OSPF Routing and Database Status

The deployment of Open Shortest Path First (OSPF) was verified to ensure complete network awareness and dynamic route propagation across the simulated topology. Using the show ip ospf database command, the following were confirmed:

- Router Link States: Verified that all nodes were active and correctly advertising their presence within Area 0.
- Network Link States: Confirmed that the routers were fully aware of the interconnecting satellite links and ground station segments.

2) GRE and IPsec Tunnel Status

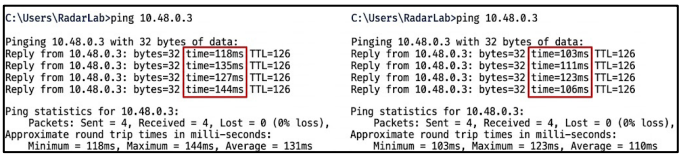
The successful establishment of encrypted tunnels was verified to ensure ASTERIX data would be properly encapsulated and protected during transit. Table 3 summarizes the outcomes from the security verification process.

TABLE 3: SECURITY VERIFICATION

Verification Command	Parameter Checked	Outcome
show interface tunnel	Line Protocol	Both Tunnel 0 and Tunnel 1 were "up," indicating operational GRE encapsulation.
	MTU and Bandwidth	Confirmed a tunnel MTU of 1414 bytes and a logical tunnel-interface bandwidth value of 8000 kbps. The actual emulated satellite-link capacity was limited to 2 Mbps using NETEM.
	Tunnel Protection	Verified that tunnel interfaces were protected via the "IPSEC_PROFILE".
show crypto isakmp sa	QM_IDLE State	Confirmed successful IKE Phase 1 negotiation, indicating active security associations.
	Connectivity	Active status verified for source-destination pairs 172.72.110.1 and 172.72.210.1.

E. Connectivity Validation

The ICMP ping test was conducted to evaluate network connectivity and measure round-trip time (RTT) between the radar sites and the Command Operations Centre (COC). The test confirmed successful communication across the GRE over IPsec tunnels, with consistent RTTs indicating operational network performance.



(a) (b)

Fig. 2. Initial ICMP Test Result, (a) RSA to COC (b) RSB to COC.

The methodology established a controlled yet realistic environment to evaluate the transition from unsecured to encrypted military communications. By systematically moving from system characterization to real-time performance validation, the study ensured that all variables—ranging from satellite-induced latency to encryption-driven processing costs—were isolated and measured. The integration of GNS3 for topology emulation, NETEM for network impairment, and Sky Display for operational verification provided a robust framework to confirm that the security enhancements did not compromise the real-time requirements of air surveillance. This structured approach ensures that the resulting data provides a reliable basis for the subsequent comparative analysis of delay and throughput.

IV. Results And Analysis

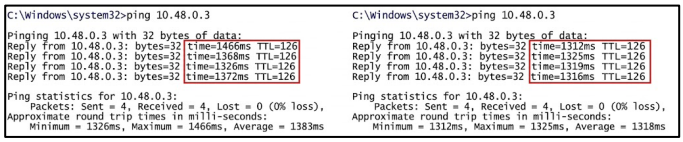
The evaluation of the air defence communication network was conducted based on three primary metrics: connectivity under satellite constraints, the efficacy of data confidentiality, and a comparative performance analysis of delay and throughput between unsecured and secured configurations.

A. Network Connectivity and Baseline Latency

Initial verification using ICMP ping tests confirmed end-to-end connectivity through the GRE over IPsec tunnels.

- **Baseline Performance**: Initial tests showed average Round-Trip Times (RTT) of 131 ms for Radar Site A (RSA) and 110 ms for Radar Site B (RSB). These RTTs exceeded standard thresholds (20–50 ms) Budiansyah & Iqbal [35].
- **Satellite Emulation**: Upon introducing XSatcom parameters via NETEM (600 ms delay, 2 Mbps bandwidth), RTT increased to 1383 ms for RSA and 1318 ms for RSB.
- **Connectivity Integrity**: Despite the high latency inherent in geostationary satellite links, the tunnels maintained 0% packet loss, confirming a stable connection for surveillance data.

Fig. 3 presents the ICMP test results under the simulated XSatcom conditions.



(a) (b)

Fig. 3. Initial ICMP Test Result with 2 Mbps bandwidth and 600ms delay (a) RSA to COC (b) RSB to COC.

B. Data Confidentiality and Integrity Verification

The second objective of this project was to simulate the secure transmission of ASTERIX data between the two remote radar sites (RSA and RSB) and the Command Operations Centre (COC). During the simulation, each radar site transmitted 2500 ASTERIX data packets through GRE over IPsec tunnels.

A critical objective was to verify the security of ASTERIX radar data during transmission.

- **Encryption Verification**: Wireshark captures confirmed the presence of **Encapsulating Security Payload (ESP)** packets, proving that IPsec encryption was correctly applied to the GRE-encapsulated traffic.
- **Payload Integrity**: At the COC, received multicast packets (239.1.1.1 and 239.2.1.1) were decrypted successfully, with all ASTERIX fields (Data Source Identifier, Time of Day, and Target Reports) remaining intact.
- **Visual Validation**: Using **Sky Display** software, target plots for RBA684 (RSA) and AXM6495 (RSB) were visualized without data loss, confirming that the secure tunnel did not compromise the usability of the surveillance data.

As shown in Fig. 4, the presence of Encapsulating Security Payload (ESP) packets in the Wireshark capture verifies that IPsec encryption was correctly applied. The source and destination IP addresses confirm packet flow from radar sites to the COC, validating the secure encapsulation of GRE traffic.

Further confirmation is provided in Fig. 5, which displays the received packets at the COC. These packets, identified by multicast IP addresses 239.1.1.1 and 239.2.1.1, demonstrate the correct reception and decryption of ASTERIX data. Key fields such as the Data Source Identifier, Time of Day, and Target Report Descriptor were found intact, confirming the preservation of data structure during transmission.

Visual validation was conducted using Sky Display software. As depicted in Fig. 6 and Fig. 7, target plots from RSA (Johor Bahru) and RSB (Kota Kinabalu) were successfully displayed on the map, confirming accurate reception and processing of ASTERIX packets at the COC.

To ensure the integrity and accuracy of the received ASTERIX surveillance data, verification was conducted using Sky Display software. The focus was on two specific targets: RBA684 from Radar Site A (RSA) and AXM6495 from Radar Site B (RSB). As shown in Fig. 8, the target RBA684, detected

by RSA in Johor Bahru, was consistently plotted without any missing data points, confirming the complete and reliable transmission of ASTERIX packets from that site.

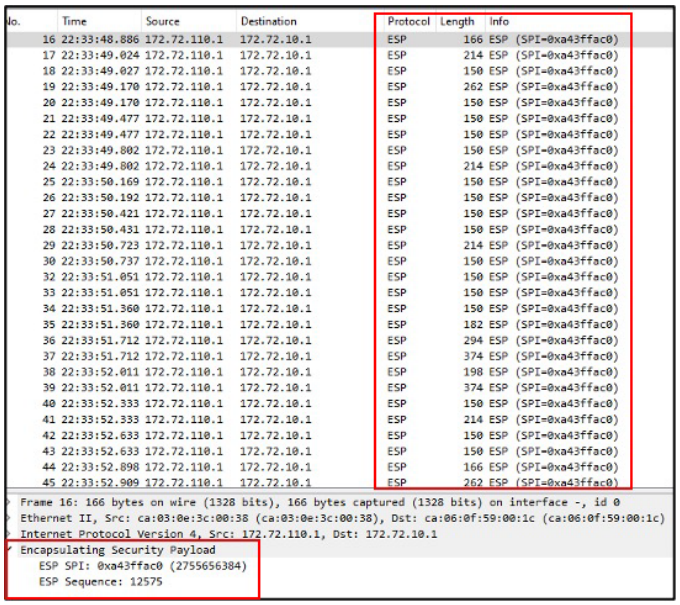


Fig. 4. Captured ESP packets.

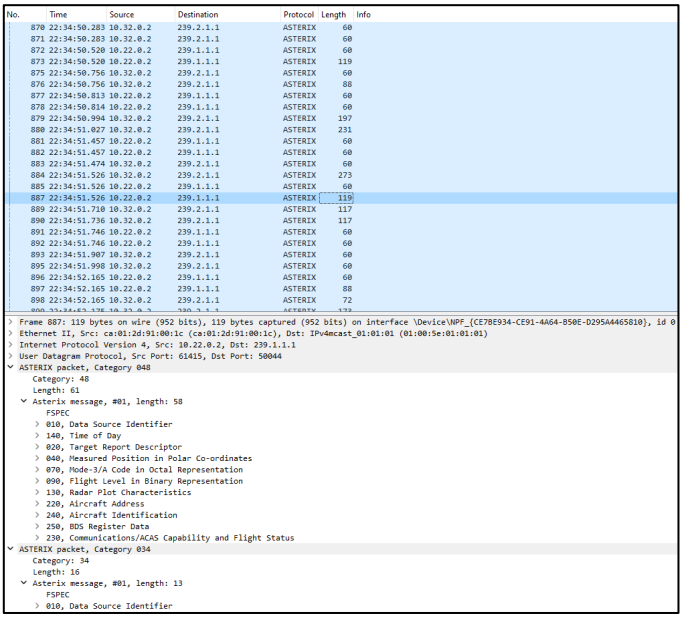


Fig. 5. Capture of received packets.

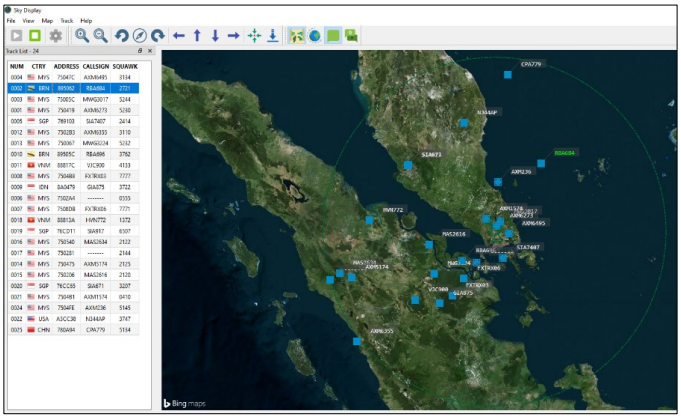


Fig. 6. Target plots for RSA.

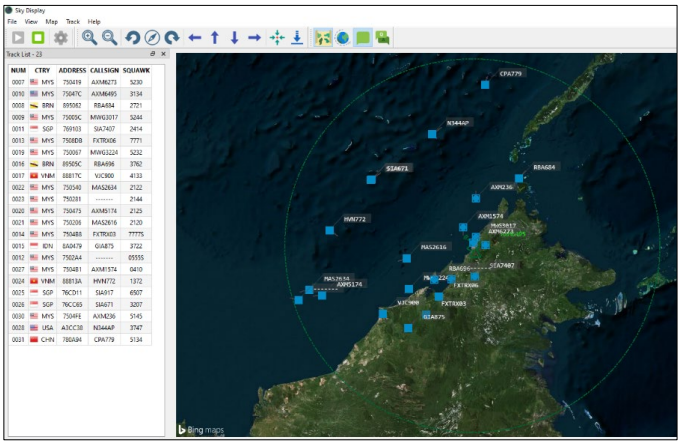


Fig. 7. Target plots for RSB.

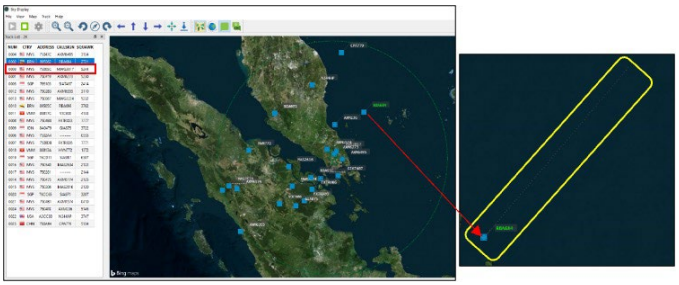


Fig. 8. Verification of target plot, RBA 684 detected by RSA.

Similarly, Fig. 9 displays the target AXM6495, detected by RSB in Kota Kinabalu. The data for this target was also plotted seamlessly, with no interruptions observed, demonstrating that the transmission from RSB was equally reliable and unaffected by packet loss.

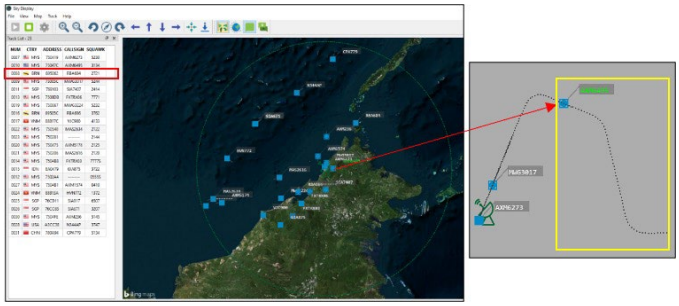


Fig. 9. Verification of target plot, AXM6495 detected by RSB.

These results, taken together with earlier ICMP and ASTERIX packet capture tests (see Fig. 10), confirm that despite high latency and limited bandwidth, the GRE over IPsec configuration maintained consistent, uninterrupted data flow. The simulated environment in GNS3, which excluded external variables such as radio frequency interference, allowed for focused analysis of the tunneling protocol's effectiveness.

Overall, the ability to consistently visualize complete target plots validates that the network successfully fulfilled the second objective of this study. The secure GRE over IPsec tunnels did not compromise performance, confirming that this method supports reliable, real-time air surveillance over a satellite-based defence communication network.

The third objective of this project is to assess the security and performance of the air defence communication network by comparing GRE-only (unsecured) and GRE over IPsec (secured) configurations under XSatcom conditions. Performance was measured in terms of data confidentiality, delay, and throughput, providing a balanced evaluation of security implementation and operational efficiency.

Captured packet analysis via Wireshark highlights the contrast in data exposure between the two configurations. In the GRE-only setup, as seen in Fig. 10, ASTERIX data, including host IPs and ports, is transmitted in plaintext, posing significant risks to data confidentiality. In contrast, the GRE over IPsec configuration shown in Fig. 11 uses Encapsulating Security Payload (ESP) to encrypt data, protecting it from interception or tampering.

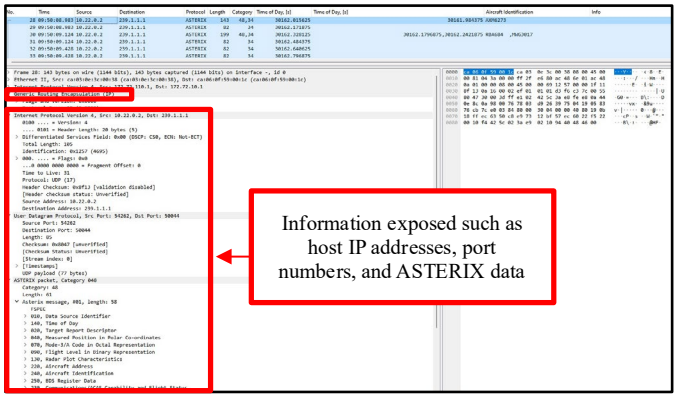


Fig. 10. Unsecured tunnel, GRE encapsulation with barely exposed information.

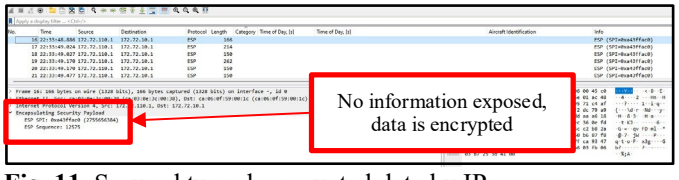


Fig. 11. Secured tunnel, encrypted data by IPsec.

While IPsec introduces some packet overhead, the confidentiality benefits far outweigh this cost, making it essential for securing sensitive surveillance data in military-grade networks.

C. *Comparative Performance Analysis*

The final objective compared the GRE-only (unsecured) and GRE over IPsec (secured) configurations.

1) *Delay vs. Packet Size*

Delay was evaluated using ICMP ping tests with varying packet sizes, for small packet sizes (32 to 500 bytes), delay differences between GRE and GRE over IPsec were minimal. However, as packet sizes increased (up to 60,000 bytes), delays rose more sharply under the secure configuration up to 2200 ms compared to 2000 ms for GRE-only. Table 4 summarizes the analysis conducted.

TABLE 4: PACKET SIZE VS DELAY

Packet Size	GRE-Only Delay	GRE over IPsec Delay	Observation
Small (<500B)	Baseline	Baseline	Minimal difference; ideal for ASTERIX.
Large (60kB)	~2000 ms	~2200 ms	~10% increase due to encryption overhead.

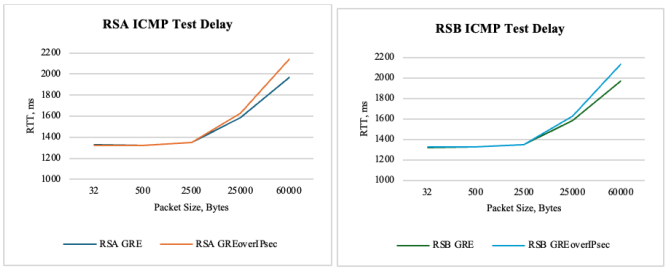


Fig. 12. Delay graph for RSA and RSB.

This increased delay is due to encryption and decryption overhead introduced by IPsec. Still, since ASTERIX packets are typically small (less than 500 bytes), the impact on operational performance is negligible. Thus, IPsec can be deployed without compromising real-time data transmission requirements.

2) *Throughput Stability*

The application-level throughput was measured during the replay of the ASTERIX traffic under both GRE-only and GRE over IPsec configurations. For Radar Site A (RSA), the average throughput decreased slightly from 39.1 kbps under the GRE-only configuration to 38.9 kbps under the GRE over IPsec configuration. For Radar Site B (RSB), the average throughput remained at 39.1 kbps for both configurations. The difference observed for RSA represents a reduction of approximately 0.5%, indicating that the encryption overhead had only a minor effect on the ASTERIX traffic rate.

The observed throughput of approximately 39 kbps represents the application-level traffic rate generated during the replay of the ASTERIX packets rather than the maximum capacity of the 2 Mbps emulated satellite link. Since ASTERIX surveillance messages are relatively small and transmitted intermittently according to the radar reporting intervals, the generated traffic did not saturate the available link bandwidth. These results indicate that GRE over IPsec maintained a stable

ASTERIX traffic rate while providing encryption for the transmitted radar data.

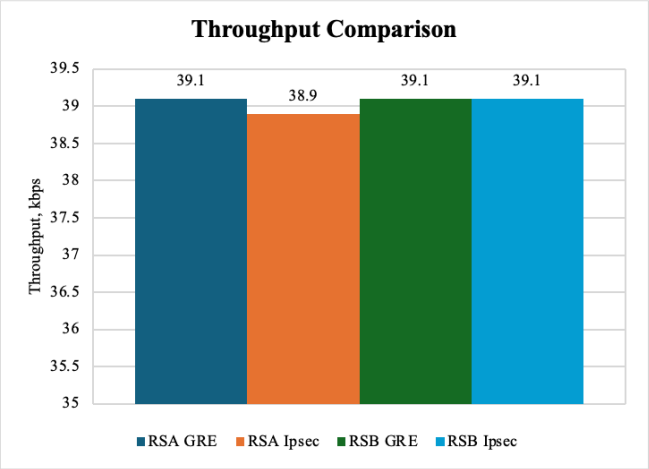


Fig. 13. Throughput performance comparison between unsecured (GRE-only) and secured (GRE over IPsec) tunnels.

The result confirms that GRE over IPsec provides strong data confidentiality while maintaining acceptable levels of delay and throughput. Although secure configurations incur slightly higher delays for large packets, the impact is minimal for typical ASTERIX transmissions. Therefore, GRE over IPsec is validated as a practical solution for secure, high-performance data transmission in air defence networks over satellite links.

Table 5 summarizes the outcomes from the study through comparative method. In terms of mission suitability, the performance gap between the two protocols is virtually non-existent in a real-world surveillance context, primarily because ASTERIX Categories 34 and 48 typically involve small message sizes of under 500 bytes. This efficiency provides a strong security justification for the transition from plaintext exposure to full AES-256 encryption; the minor processing overhead is a necessary trade-off to mitigate critical threats, such as man-in-the-middle attacks on the satellite link. It should be noted that part of the measured latency 1318 to 1383 ms under satellite conditions, may be attributed to software emulation overhead associated with GNS3 and virtualized routers. In operational military environments, dedicated hardware routers equipped with cryptographic acceleration or FPGA-based IPsec processing are expected to reduce processing delay and improve throughput performance compared with software-based implementations.

The comparative analysis depicted in Table 5, reveals that while the GRE over IPsec configuration introduces additional processing requirements, it maintains the high-performance standards necessary for mission-critical air surveillance.

TABLE 5: COMPARATIVE ANALYSIS ON PERFORMANCE METRICS

Metric	GRE-Only (Unsecured)	GRE over IPsec (Secured)	Impact/ Observation
Data Confidentiality	None; Host IPs, ports, and ASTERIX payloads visible in plaintext.	High; Full encryption using ESP (AES-256).	IPsec effectively hides sensitive military data.
Average Throughput (RSA)	39.1 kbps.	38.9 kbps.	Negligible decrease (0.5%) in transmission rate.
Average Throughput (RSB)	39.1 kbps.	39.1 kbps.	No measurable impact on throughput for Site B.
Latency (Small Packets <500B)	Minimal/ Baseline.	Minimal/ Baseline.	No significant operational delay for standard ASTERIX packets.
Latency (Large Packets 60kB)	~2000 ms.	~2200 ms.	~10% increase due to encryption/ decryption overhead.
Packet Integrity	Not Guaranteed.	Guaranteed via SHA-256 Hashing.	Prevents unauthorized tampering or data injection.

The present study compares GRE-only and GRE over IPsec configurations because these represent the two practical deployment options considered within the evaluated air defence network architecture. Native XSatcom transmission without GRE encapsulation and an IPsec-only configuration were not included in the current experimental scope. Future studies should compare Native XSatcom, GRE-only, IPsec-only, and GRE over IPsec under identical satellite-link conditions to provide a more comprehensive assessment of delay, throughput, packet loss, and jitter.

V. CONCLUSION

This study evaluated the use of GRE over IPsec to secure ASTERIX CAT 34 and CAT 48 radar communications over a simulated XSatcom link. The results show that AES-256-based GRE over IPsec protected the confidentiality of the transmitted radar data while introducing only a small reduction in application-level throughput and a limited increase in delay for the small packet sizes typically associated with ASTERIX traffic. Despite satellite-induced round-trip latency exceeding one second, the tested configuration maintained stable communication performance and consistent throughput.

From a scientific perspective, this study provides empirical evidence on the security–performance trade-off of GRE over IPsec for ASTERIX radar traffic under simulated GEO satellite constraints. From a practical perspective, the evaluated architecture provides a reference configuration for securing communications between remote radar sites and a Command Operations Centre through an XSatcom backup link.

The findings are limited to the GNS3 and VMware-based simulation environment used in this study. Future work should consider to include field testing using dedicated networking hardware to assess the effects of radio-frequency propagation loss, environmental variability, and hardware-based cryptographic acceleration. Future studies should also compare Native XSatcom, GRE-only, IPsec-only, and GRE over IPsec configurations under identical network conditions and include systematic jitter measurements to provide a more complete assessment of packet timing variation.

The authors declare that there is no conflict of interest

regarding the publication of this paper. The ASTERIX packet datasets and network configuration files used in this study contain operationally sensitive information. Therefore, they are not publicly available but may be provided upon reasonable request and subject to approval from the relevant authorities.

VI. ACKNOWLEDGMENT

The authors would like to thank the Universiti Teknologi MARA, 40450 Selangor, Malaysia for the support in publishing this paper.

REFERENCES

[1] I. Petrović, M. Kankaraš, and K. Cvetković, "Significance and prospects of the development of air defence system," Vojno delo, vol. 67, no. 6, pp. 86–98, 2015.

[2] G. Kołata, "Airbase as Defended Asset for Air Defense," Safety & Defense, vol. 5, no. 1, pp. 37–45, 2019.

[3] Ministry of Defence Malaysia, Defence White Paper 2020–2030, Kuala Lumpur, Malaysia: Ministry of Defence Malaysia, 2020. [Online]. Available: https://www.mod.gov.my/index.php/en/information/defence-white-paper. [Accessed: Aug. 13, 2026].

[4] Z. Shaharan, "The Launching of MEASAT-3B at Kourou, French Guiana – 11 September 2014 (Local Time)," Embassy of Malaysia, Paris: Ministry of Foreign Affairs, Malaysia, 2014. [Online]. Available: https://www.kln.gov.my/web/fra_paris/post/the-launching-of-measat-3b-at-kourou-french-guiana-11-september-2014-local-time. [Accessed: Aug. 13, 2026].

[5] Y. Firmansyah, N. Rahayu, Y. Prabowo, I. N. Y. Putro, and F. Kurniawan, "Quality of service (QoS) analysis for real-time telemetry by IP satellite communication," in 2020 International Conference on Radar, Antenna, Microwave, Electronics, and Telecommunications (ICRAMET), IEEE, 2020, pp. 18–21.

[6] G. Romain, P. David, P. Guillaume, and K. Nicolas, "Recommendations on using VPN over SATCOM," arXiv preprint arXiv:2111.04586, 2021.

[7] J. K. Pedersen, M. Bøchman, and W. Meng, "Security analysis in satellite communication based on geostationary orbit," in 2022 19th Annual International Conference on Privacy, Security & Trust (PST), IEEE, 2022, pp. 1–10.

[8] K. A. Ogudo, "Analyzing generic routing encapsulation (GRE) and IP Security (IPSec) tunneling protocols for secured communication over public networks," in 2019 International Conference on Advances in Big Data, Computing and Data Communication Systems (icABCD), IEEE, 2019, pp. 1–9.

[9] J. Li and M. Zhou, "Research on VPN in Experimental Simulation Environment Based on GRE and IPSec," in Proceedings of the 6th International Conference on Robotics and Artificial Intelligence, 2020, pp. 220–224.

[10] W. Penaflor Rey and K. W. J. Dugang Rey, "Designing Secure and Scalable end-to-end Private Network Connections between sites via Overlay Tunnels," in The 2022 5th International Conference on Electronics, Communications and Control Engineering, 2022, pp. 50–56.

[11] M. R. Uddin, N. A. Evan, M. R. Alam, and M. T. Arefin, "Analysis of Generic Routing Encapsulation (GRE) over IP Security (IPSec) VPN Tunneling in IPv6 Network," in UBICNET 2021, Springer, 2021, pp. 3–15.

[12] S. Budiyanto and D. Gunawan, "Comparative Analysis of VPN Protocols at Layer 2 Focusing on Voice over Internet Protocol," IEEE Access, 2023.

[13] O. A. Alausa, S. A. Arekete, M. O. Odim, A. O. Oguntunde, and A. O. Ogunde, "VoIP Codec Performance Evaluation on GRE with IPsec over IPv4 and IPv6," Advances in Science, Technology and Engineering Systems Journal, vol. 6, no. 5, pp. 260–266, 2021.

[14] W. He et al., "Design of Dual-link Shared GRE over IPSec VPN on P2MP Networks," in 2023 IEEE ICPECA, 2023, pp. 1781–1783.

[15] D.-L. Murariu and P. Ciotirnae, "Performance Evaluation of the VoIP Networks Using Tunneling Techniques," in ECAI 2019, IEEE, 2019, pp. 1–4.

[16] S. Budiyanto and L. M. Silalahi, "Analysis QoS VoIP using GRE+ IPSec Tunnel and IPIP Based on Session Initiation Protocol," in IC2IE 2022, IEEE, 2022, pp. 47–54.

[17] Z. C. S. Stankovic, D. Drajic, R. Petrovic, and M. Peric, "Implementation of GRE Tunelling on low cost SoM," presented at TELFOR 2022, 2022.

[18] K. F. Mahmmod, M. M. Azeez, and M. A. Ahmed, "IPsec cryptography for data packets security within vpn tunneling networks communications," in ICELTICs 2020, IEEE, 2020, pp. 1–8.

[19] Z. Xu and J. Ni, "Research on network security of VPN technology," in ICISE-IE 2020, IEEE, 2020, pp. 539–542.

[20] V. Hashiyana, T. Haiduwa, N. Suresh, A. Bratha, and K. O. Flavia, "Design and Implementation of an IPSec Virtual Private Network: A Case Study at the University of Namibia," in IST-Africa 2020, IEEE, 2020, pp. 1–6.

[21] Z. Basit, M. Tabassum, T. Sharma, M. Furqan, and A. Q. Md, "Performance analysis of OSPF and EIGRP convergence through IPsec tunnel using Multi-homing BGP connection," Materials Today: Proceedings, vol. 62, pp. 4853–4861, 2022.

[22] E. Darmawan, S. Budiyanto, and L. M. Silalahi, "QoS Analysis on VoIP with VPN using SSL and L2TP IPSec Method," in COMNETSAT 2022, IEEE, 2022, pp. 130–136.

[23] M. Juma, A. A. Monem, and K. Shaalan, "Hybrid end-to-end VPN security approach for smart IoT objects," Journal of Network and Computer Applications, vol. 158, p. 102598, 2020.

[24] I. Nurhaida and Ngadiyono, "Quality of service for traffic monitoring system based on static routing using EoIP tunnel over IPSec," in Asia Pacific Information Technology Conference, 2019, pp. 91–99.

[25] F. W. Dharma, "Enhancing branch office network availability using cloud EoIP gateway," Procedia Computer Science, vol. 179, pp. 574–581, 2021.

[26] A. I. Haris, R. A. Ferianda, and A. I. Basuki, "QoS Analysis of Site-to-Site VPN and Its Integration Potential for Securing Communication on Electric Vehicles," in ICCCIA 2022, 2022, pp. 25–28.

[27] S. T. A. T. Thein, "Comparative Analysis of Site-to-Site Layer 2 Virtual Private Networks," presented at ICCA 2020, Myanmar, 2020.

[28] K. Gaur et al., "A survey of virtual private LAN services (VPLS): Past, present and future," Computer Networks, vol. 196, p. 108245, 2021.

[29] D. Crawshaw, "Everything VPN is New Again: The 24-year-old security model has found a second wind," Queue, vol. 18, no. 5, pp. 54–66, 2020.

[30] C. A. R. Goyzueta, J. E. C. De La Cruz, and C. D. Cahuana, "VPNoT: end to end encrypted tunnel based on OpenVPN and Raspberry Pi for IoT security," in ICECCME 2021, IEEE, 2021, pp. 1–5.

[31] M. Kang, S. Park, and Y. Lee, "A survey on satellite communication system security," Sensors, vol. 24, no. 9, Art. no. 2897, 2024, doi: 10.3390/s24092897.

[32] F. Casaril and L. Galletta, "Securing SatCom user segment: A study on cybersecurity challenges in view of IRIS²," Computers & Security, vol. 140, Art. no. 103799, 2024, doi: 10.1016/j.cose.2024.103799.

[33] S. Ansong, W. Rankothge, S. Sadeghi, H. Mohammadian, F. B. Rashid, and A. A. Ghorbani, "Role of cybersecurity for a secure global communication eco-system: A comprehensive cyber risk assessment for satellite communications," Computers & Security, vol. 149, Art. no. 104156, 2025, doi: 10.1016/j.cose.2024.104156.

[34] K. R. Kurose, Computer networking: A top-down approach, J. Keith W. Ross, 2017, p. 601.

[35] A. Budiansyah and M. Iqbal, "A Testing Packet Delay Variation and Packet Loss Problem on Local Area Network Based on ITU-T Standard," in IOP Conference Series: Materials Science and Engineering, vol. 506, no. 1, p. 012049, 2019.